Números enteros - Divisibilidad

Elementos de Álgebra
Segundo Cuatrimestre 2022

Mg. María del Carmen Vannicola

Facultad de Informática
Departamento de Matemática

Definición

Sean $a, b \in \mathbb{Z}$. Se dice que **"a" divide a "b"** *si y sólo si existe $k \in \mathbb{Z}$ tal que $b = k \cdot a$.*

Si "a" divide a "b" notaremos $a|b$. Es decir,

$$a|b \iff \exists\, k \in \mathbb{Z} /\, b = k \cdot a$$

Si a divide a b diremos que a **es un divisor de** b, o que a **es un factor de** b, o que b **es divisible por** a, o que b **es un múltiplo de** a.

Si "a" no divide a "b" notaremos $a \nmid b$, lo que equivale a

$$\sim (\exists\, k \in \mathbb{Z} /\, b = k \cdot a) \iff \forall k \in \mathbb{Z} : \; b \neq k \cdot a$$

Ejemplos

- $4|132$ ya que $132 = 33 \cdot 4$
- $23|0$ pues $0 = 0 \cdot 23$

- $7 | -245$

$$\begin{array}{r|l} 245 & 7 \\ \cline{2-2} 35 & 35 \\ \underline{0} & \end{array}$$

$245 = 35 \cdot 7$ entonces $-245 = (-35) \cdot 7$

- Mostremos que $-3 \nmid 14$

  Supongamos que $-3|14$, es decir, que existe $k \in \mathbb{Z}$ tal que $14 = -3k$ entonces

  si $k = 0$, luego $14 = -3 \cdot 0$, es decir, $14 = 0$, absurdo;

  si $k \geq 1$ inferimos que $-3k \leq -3$, entonces $14 \leq -3$, absurdo;

  si $k = -1, -2, -3, -4 \quad -3k = 3, 6, 9, 12$, de lo que deducimos,

  $$14 = 3, \ 6, \ 9, \ 12, \ \text{absurdo};$$

  si $k \leq -5, \quad -3k \geq 15$, luego $14 \geq 15$, absurdo;

  estas contradicciones provienen de suponer que $-3|14$, esto es, $-3 \nmid 14$.

Relación divide - Propiedades

Proposición

Sean $a, b, c \in \mathbb{Z}$. Se verifican las siguientes propiedades

1. *Reflexiva:* $\forall a \in \mathbb{Z}: \ a|a$
2. $\forall a \in \mathbb{Z}: \ a|0, \ 1|a, \ -1|a$
3. *Si* $a|b$ *entonces* $a|-b, \ -a|b, \ -a|-b$
4. *Si a divide a b entonces valor absoluto de b es múltiplo del valor absoluto de a*
5. $a|b$ *y* $b|a$ *es equivalente a* $|a| = |b|$
6. *Transitiva: si* $a|b$ *y* $b|c$ *entonces* $a|c$

Demostración

1. $\forall a \in \mathbb{Z}: \ \exists 1 \in \mathbb{Z} / \ a = 1 \cdot a$ entonces
$$\forall a \in \mathbb{Z}: \ a|a$$
2. Demostraremos que $a|0, \ \forall a \in \mathbb{Z}$. El resto de las proposiciones del item 2 se proponen como ejercicios

   Como $\exists 0 \in \mathbb{Z} / \ 0 = 0 \cdot a$ entonces $a|0, \ \forall a \in \mathbb{Z}$

Relación divide - Propiedades

3. Probaremos que si $a|b$ entonces $a|-b$. El resto de la demostración se deja como ejercicio.

$H_1)$ $a, b \in \mathbb{Z}$ $\quad H_2)$ $a|b$ $\quad T)$ $a|-b$

Demostración: (método directo)

$$a|b \overset{(1)}{\Longrightarrow} \exists\, k \in \mathbb{Z} /\ b = ka \Longrightarrow \exists\, k \in \mathbb{Z} / -b = -ka \Longrightarrow$$

$$\Longrightarrow \exists\, k \in \mathbb{Z} / -b = (-k)a \Longrightarrow \exists -k \in \mathbb{Z} / -b = (-k)a \overset{(1)}{\Longrightarrow} a|-b$$

Referencia: (1) Definición de la relación divide.

4. Demostremos que, si a divide a b entonces valor absoluto de b es múltiplo del valor absoluto de a.

$H_1)$ $a, b \in \mathbb{Z}$ $\quad H_2)$ $a|b$ $\quad T)$ $\exists\, k \in \mathbb{Z} /\ |b| = k|a|$(Por la definición de múltiplo)

Demostración: (método directo)

$$a|b \overset{(1)}{\Longrightarrow} \exists t \in \mathbb{Z} /\ b = t \cdot a \Longrightarrow \exists t \in \mathbb{Z} /\ |b| = |t \cdot a| = |t| \cdot |a| \Longrightarrow$$

$$\Longrightarrow \exists\, k \in \mathbb{Z},\ k = |t| /\ |b| = k|a|$$

Referencia: (1) Definición de la relación divide.

5. En primer lugar probemos la implicación $a|b \ \wedge \ b|a \implies |a| = |b|$

$H_1)\ a, b \in \mathbb{Z}$ $\quad H_2)\ a|b$ $\quad H_3)\ b|a$ $\quad T)\ |a| = |b|$

Demostración: (método directo)

$$a|b \ \wedge \ b|a \stackrel{(1)}{\implies} \exists\, k \in \mathbb{Z}/\ b = ka \ \wedge \ b|a \stackrel{(1)}{\implies}$$

$$\implies \exists\, k \in \mathbb{Z}/\ b = ka \ \wedge \ \exists\, t \in \mathbb{Z}/\ a = tb \implies \exists\, k, t \in \mathbb{Z}/\ b = ka \ \wedge \ a = tb \implies$$

$$\implies \ \exists\, k, t \in \mathbb{Z}/\ b = k(tb) = (kt)b \implies \exists\, k, t \in \mathbb{Z}/\ kt = 1$$

Si $kt = 1$, como k y t son enteros por H_1), entonces $k = t = 1 \ \vee \ k = t = -1$.

Si $k = t = 1$, como $b = ka \ \wedge \ a = tb$ entonces reemplazando obtenemos

$$b = a \ \wedge \ a = b \implies a = b \implies |a| = |b|$$

Si $k = t = -1$ reemplazando en $b = ka \ \wedge \ a = tb$ deducimos

$$b = -a \ \wedge \ a = -b \implies -b = a \ \wedge \ a = -b \implies a = -b \implies |a| = |b|$$

Luego, hemos probado que: $a|b \ \wedge \ b|a \implies |a| = |b| \quad (2)$

Referencia: (1) Definición de la relación divide

Relación divide - Propiedades

Demostremos ahora que, $|a| = |b| \implies a|b \ \wedge \ b|a$

$H_1)\ a, b \in \mathbb{Z}$ $\qquad$ $H_2)\ |a| = |b|$ $\qquad$ $T)\ a|b \ \wedge \ b|a$

Demostración: (método directo)

$$|a| = |b| \overset{(3)}{\Longrightarrow} a = b \ \vee \ a = -b \implies a = b \ \vee \ -a = b \implies$$

$$\implies b = 1 \cdot a \ \vee \ b = (-1)a \implies$$

$$\implies \exists\, k \in \mathbb{Z},\ k = 1 \,/\, b = k \cdot a \vee \exists\, t \in \mathbb{Z},\ t = -1 \,/\, b = t \cdot a \overset{(4)}{\Longrightarrow} a|b \vee a|b \overset{(5)}{\Longrightarrow} a|b$$

Análogamente se prueba que, $|a| = |b| \implies b|a$

Demostramos entonces que, $|a| = |b| \implies a|b \ \wedge \ b|a \quad (6)$

De (2) y (6) deducimos que

$$a|b \ \wedge \ b|a \iff |a| = |b|$$

Referencia: (3) Propiedad de valor absoluto: $|x| = |y| \iff x = \pm y$

(4) Definición de la relación divide.

(5) Idempotencia de la disyunción.

Relación divide - Propiedades

6. Probemos que $a|b \ \wedge \ b|c \implies a|c$

$H_1)\ a, b, c \in \mathbb{Z}$ $\quad H_2)\ a|b$ $\quad H_3)\ b|c$ $\quad T)\ a|c$

Demostración: (método directo)

$$a|b \ \wedge \ b|c \overset{(1)}{\implies} \exists\, k \in \mathbb{Z} /\ b = ka \ \wedge \ \exists\, t \in \mathbb{Z} / c = tb \implies$$

$$\implies \exists\, k, t \in \mathbb{Z}/\ b = ka \ \wedge c = tb \implies \exists\, k, t \in \mathbb{Z}/\ c = t(ka) = (tk)a \implies$$

$$\implies \exists\, h \in \mathbb{Z},\ h = tk/\ c = ha \overset{(1)}{\implies} a|c$$

Demostramos que, si $a|b \ \wedge \ b|c$ entonces $a|c$

Referencia: (1) Definición de la relación divide

Relación divide - Propiedades

Proposición

Sean $a, b, c \in \mathbb{Z}$. Se verifican las siguientes propiedades

1. *Si $b \neq 0$ y a es un divisor de b entonces $1 \leq |a| \leq |b|$*
2. $a|b \ \wedge \ a|c \implies a|bx + cy, \ \forall x, y \in \mathbb{Z}$
3. $a|b \implies ac|bc$
4. *Si $c \neq 0$ entonces $ac|bc \implies a|b$*
5. $a|b \implies a|bc$
6. $\forall n \in \mathbb{N} : \ a|b \implies a|b^n$

1. $H_1)\ b \neq 0$ $\qquad$ $H_2)\ a|b$ $\qquad$ $T)\ 1 \leq |a| \leq |b|$

   Demostración: (método directo)

   $a|b \overset{(1)}{\implies} \exists\, k \in \mathbb{Z}/\ b = k \cdot a \implies \exists\, k \in \mathbb{Z}/\ |b| = |k \cdot a| = |k| \cdot |a|$

   Como $b \neq 0$, $k \neq 0$ entonces $1 \leq |k|$, luego $|a| \leq |k| \cdot |a|$, es decir, $|a| \leq |b|$

   Como $a|b$ y $b \neq 0$ entonces $a \neq 0$, luego $1 \leq |a|$. De lo que deducimos

$$1 \leq |a| \leq |b|$$

Relación divide - Propiedades

2. $H_1)\ x,\ y \in \mathbb{Z}$ $\quad H_2)\ a|b$ $\quad H_3)\ a|c$ $\quad T)\ a|bx+cy$

   Demostración: (método directo)

   $$a|b \ \wedge \ a|c \xrightarrow{(1)} \exists\, k,t \in \mathbb{Z}/\ b = ka \ \wedge \ c = ta \implies$$

   $$\implies \exists\, k,t \in \mathbb{Z}/\ bx = (ka)x = (kx)a \ \wedge \ cy = (ta)y = (ty)a \implies$$

   $$\implies \exists\, k,t \in \mathbb{Z}/\ bx + cy = (kx)a + (ty)a = (kx+ty)a \implies$$

   $$\overset{H_1)}{\implies} \exists\, h \in \mathbb{Z},\ h = kx + ty/\ bx + cy = ha \xrightarrow{(1)} a|bx+cy$$

   Luego $a|b \ \wedge \ a|c \implies a|bx+cy$, cualesquiera sean $x, y \in \mathbb{Z}$

   Referencia: (1) Definición de la relación divide

3. $H_1)\ a|b$ $\quad T)\ ac|bc$

   Demostración: (método directo)

   $$a|b \xrightarrow{(1)} \exists\, k \in \mathbb{Z}/\ b = ka \implies \exists\, k \in \mathbb{Z}/\ bc = (ka)c = k(ac) \xrightarrow{(1)} ac|bc$$

   Luego, $\forall c \in \mathbb{Z}:\ a|b \implies ac|bc$

   Referencia: (1) Definición de la relación divide

4. $H_1)\ c \neq 0 \qquad H_2)\ ac|bc \qquad T)\ a|b$

   Demostración: (método directo)

   $$ac|bc \xRightarrow{(1)} \exists k \in \mathbb{Z}/\ bc = k(ac) \implies \exists k \in \mathbb{Z}/\ bc = (ka)c \xRightarrow{H_1)}$$

   $$\implies \exists k \in \mathbb{Z}/\ b = k \cdot a \implies a|b$$

   Luego, $\forall c \in \mathbb{Z},\ c \neq 0 :\ ac|bc \implies a|b$

   Referencia: (1) Definición de la relación divide

5. $H_2)\ a|b \qquad T)\ a|bc$

   Demostración: (método directo)

   $$a|b \xRightarrow{(1)} \exists k \in \mathbb{Z}/\ b = ka \implies \exists k \in \mathbb{Z}/\ bc = kac = (kc)a \implies$$

   $$\implies \exists t \in \mathbb{Z},\ t = kc/\ bc = ta \implies a|bc$$

   Luego, $\forall c \in \mathbb{Z} :\ a|bc$

   Referencia: (1) Definición de la relación divide

6. Consideremos $p(n): \; a|b \implies a|b^n$.

   Haremos la demostración utilizando el método de inducción completa

   Probemos que $p(1)$ es verdadera. Como

   $$p(1): \; a|b \implies a|b^1$$

   $p(1)$ es verdadera por ser una tautología lógica

   Demostremos que si $k \in \mathbb{N}$ entonces $p(k) \implies p(k+1)$ es verdadera

   Hi) $p(k): \; a|b \implies a|b^k$

   T) $p(k+1): \; a|b \implies a|b^{k+1}$

   Demostración:

   $a|b \overset{Hi)}{\implies} a|b^k \overset{(Item\ 5)}{\implies} a|b^k b \implies a|b^{k+1}$

   Como $p(1)$ y $p(k) \implies p(k+1)$ son verdaderas, si $k \in \mathbb{N}$ entonces

   $$\forall n \in \mathbb{N}: \; a|b \implies a|b^n$$

Relación divide - Propiedades

Observaciones

- Hemos probado que si $a|b$ y $a|c$ entonces $a|xb + yc$, cualesquiera sean $x, y \in \mathbb{Z}$

  En particular, si tomamos $x = y = 1$ ó $x = 1$ e $y = -1$, tenemos que

  $$\text{si } a|b \text{ y } a|c \text{ entonces } a|b + c \text{ y } a|b - c$$

- En cambio que $a|b + c$ no implica que $a|b$ ó $a|c$

  Si consideramos $a = 5$, $b = 2$ y $c = 3$ tenemos que

  $$5|2 + 3 \;\wedge\; 5 \nmid 2 \;\wedge\; 5 \nmid 3$$

- Análogamente $a|b - c$ no implica que $a|b$ ó $a|c$

  Si tomamos $a = 3$, $b = 4$ y $c = 1$ tenemos que

  $$3|4 - 1 \;\wedge\; 3 \nmid 4 \;\wedge\; 3 \nmid 1$$

Relación divide - Propiedades

- Utilizando las propiedades anteriores podemos asegurar que se verifica

$$\text{si} \quad a|b+c \quad \text{y} \quad a|b \quad \text{entonces} \quad a|c$$

En efecto, $a|b+c \ \wedge \ a|b \implies a|(b+c)-b \implies a|c$

- La recíproca de la proposición

$$a|b \ \wedge \ a|c \implies a|bc$$

es falsas, es decir, la proposición

$$\text{si} \quad a|bc \quad \text{entonces} \quad a|b \quad \text{y} \quad a|c$$

es falsa

También es falsa la proposición

$$\text{si} \quad a|bc \quad \text{entonces} \quad a|b \quad \text{ó} \quad a|c,$$

ya que si $a = 6, \ b = -2 \ \text{ y } \ c = 3$ entonces

$$6|(-2)3 \quad \text{pero} \quad 6 \nmid -2 \quad \text{y} \quad 6 \nmid 3$$

Algoritmo de la división entera

Teorema

Dados dos enteros a y b, $b \neq 0$ existen enteros q y r; llamados respectivamente el cociente y el resto de dividir a por b, unívocamente determinados tales que:

$$a = bq + r \quad con \;\; 0 \leq r < |b|.$$

Observaciones

- El resto de dividir a por b es cero equivale a que $b|a$

$$b|a \iff \exists\, k \in \mathbb{Z}/\; a = kb \iff \exists\, k \in \mathbb{Z}/\; a = kb + 0$$

- Que $b \nmid a$ es equivalente a que el resto de la división de a por b no es nulo, esto es, $\exists\, q, r \in \mathbb{Z}/$

$$a = qb + r, \;\; 0 < r < |b|$$

Por ejemplo $2 \nmid a$ si y sólo si $\exists\, q, r \in \mathbb{Z}/a = 2q + r,\; 0 < r < 2$, es decir,

$$\exists\, q \in \mathbb{Z}/a = 2q + 1$$

- $3 \nmid a$ equivale a $\exists\, q, r \in \mathbb{Z}/a = 3q + r,\ 0 < r < 3$, esto es,

$$\exists\, q \in \mathbb{Z}/a = 3q + 1 \quad \vee \quad a = 3q + 2$$

- En general $b \nmid a$ si y sólo si $\exists\, q, r \in \mathbb{Z}/a = bq + r,\ 0 < r < |b|$, es decir,

$$\exists\, q \in \mathbb{Z}/a = bq+1 \vee a = bq+2 \vee \ldots \vee a = bq+(|b|-2) \vee a = bq+(|b|-1)$$

Ejemplo

Hallar el cociente y el resto de dividir 830 *por* 13*. Y utilizando estos resultados hallar el cociente y el resto de dividir* 830 *por* -13 *y* -830 *por* 13

$$\begin{array}{r|l} 830 & 13 \\ \cline{2-2} 50 & 63 \\ \underline{11} & \end{array}$$

$830 = 13(63) + 11$, como $0 \leq 11 < 13$

entonces el cociente de dividir a 830 por 13

es 63 y el resto es 11

Algoritmo de la división entera - Ejemplos

Vimos que: $830 = 13(63) + 11$, como $0 \leq 11 < 13$

$$830 = (-13)(-63) + 11 \text{ y } 0 \leq 11 < |-13| \text{ entonces}$$

el cociente de dividir a 830 por -13 es -63 y el resto es 11

$$\begin{aligned} -830 &= -(13(63) + 11) = 13(-63) - 11 = 13(-63) - 11 + 13 - 13 = \\ &= (13(-63) - 13) + (-11 + 13) = 13(-64) + 2 \end{aligned}$$

$$-830 = 13(-64) + 2 \quad \text{y} \quad 0 \leq 2 < 13 \text{ entonces}$$

el cociente de dividir a -830 por 13 es -64 y el resto es 2

Ejemplo

Analizar la verocidad de la siguiente proposición:
"si el resto de dividir a "a" por 7 es 4 entonces el resto de dividir a "$3a + 13$" por -7 también es 4".

Como el resto de dividir a "a" por 7 es 4 entonces

$$\exists\, q \in \mathbb{Z} / \; a = 7q + 4$$

Expresemos $3a + 13$ como un múltiplo de -7, más un resto

$$\begin{aligned} 3a + 13 &= 3(7q + 4) + 13 = (3 \cdot 7)q + 12 + 13 = (-7)(-3)q + 25 = \\ &= (-7)(-3q) + 21 + 4 = (-7)(-3q - 3) + 4 \end{aligned}$$

como $-3q - 3 \in \mathbb{Z}$ y $0 \leq 4 \leq |-7|$ entonces

el resto de dividir a $3a + 13$ por -7 es 4

Ejemplo

Demostremos que los posibles restos de dividir a $-a^2+1$ *por* 4 *son* 0 *ó* 1, *si* $-4 \nmid a$

Observemos que $-4 \nmid a$ si y sólo si $4 \nmid a$ y esto es equivalente a

$$\exists k \in \mathbb{Z}/ \ a = 4k+1 \ \vee \ a = 4k+2 \ \vee \ a = 4k+3$$

Si $a = 4k+1$ entonces

$$-a^2+1 = -(4k+1)^2+1 = -(16k^2+8k+1)+1 = -16k^2-8k = 4(-4k^2-2k)$$

Luego existe $q \in \mathbb{Z}, \ q = -4k^2-2k / \ -a^2+1 = 4q$ entonces

4 divide a $-a^2+1$, es decir, el resto de dividir a $-a^2+1$ por 4 es cero.

Si $a = 4k+2$ entonces

$$\begin{aligned} -a^2+1 &= -(4k+2)^2+1 = -(16k^2+16k+4)+1 = -16k^2-16k-3 = \\ &= 4(-4k^2-4k)-3+4-4 = 4(-4k^2-4k)+(-3+4)-4 = \end{aligned}$$

$$-a^2+1 = 4(-4k^2-4k) + (-3+4) - 4 = 4(-4k^2-4k-1)+1$$

Luego existe $s \in \mathbb{Z},\ s = -4k^2-4k-1 /\ -a^2+1 = 4s+1 \quad \text{y} \quad 0 \leq 1 < |4|$, esto es,

el resto de dividir a $-a^2+1$ por 4 es uno.

Si $a = 4k+3$ entonces

$$-a^2+1 = -(4k+3)^2+1 = -(16k^2+24k+9)+1 = -16k^2-24k-9+1 = 4(-4k^2-6k-2)$$

Luego existe $m \in \mathbb{Z},\ m = -4k^2-6k-2 /\ -a^2+1 = 4m$, es decir,

el resto de dividir a $-a^2+1$ por 4 es cero.

Hemos probado que

si $-4 \nmid a$ entonces el resto de dividir $-a^2+1$ por 4 es cero o es uno